What is claimed is:

1. A method of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising the steps of:

a. defining an intermediate sequence of bits that said source sequence of bits is transformed into with a configuration of a Benes network,;

b. determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits; and

c. repeating steps a. and b. using said determined intermediate sequence of bits from step b. as said source sequence of bits in step a. until a desired sequence of bits is obtained,

wherein the determined permutation instructions form a permutation instruction sequence.

2. The method of claim 1 wherein said Benes network comprises two butterfly networks of the same size connected back-to-back.

3. The method of claim 1 wherein the permutation instruction comprises an opcode indicating the configuration of said Benes network, a reference to a source register which contains said source sequence of bits, and a reference to one or more configuration registers which contain configuration bits, and optionally a reference to a destination register to which said intermediate sequence of bits or said desired sequence of bits is placed.

4. The method of claim 3 wherein said opcode comprises a set of parameters, a first parameter indicating a first basic operation and a second parameter indicating a second basic operation.

5. The method of claim 3 wherein a first set of said configuration bits determines movement of said source sequence of bits in said source register to said intermediate sequence of bits and a

second set of a subsequent intermediate sequence of bits or said configuration bits determines movement of said intermediate sequence of bits into said destination register.

6. The method of claim 5 wherein said first basic operation is specified by parameter m_1, wherein 2^{m_1} is a distance between conflict pairs of a stage of said Benes network and said second basic operation is specified by parameter m_2, wherein 2^{m_2} is a distance between conflict pairs of a stage of said Benes network.

7. The method of claim 3 including a plurality of sets of said configuration bits, wherein a first set of said configuration bits determines movement of said source sequence of bits in said source register to said intermediate sequence of bits during said first operation and a second set of said configuration bits determines movement of said intermediate sequence of bits into said destination register or a second intermediate sequence of bits during said second operation.

8. The method of claim 4 wherein said opcode comprises a plurality of parameters with each of said parameters indicating which said stage in a Benes network is used.

9. The method of claim 7 wherein each of said configuration bits is applied to a pair of conflict outputs of said Benes network.

10. The method of claim 5 wherein said permutation instruction is assigned to two or more stages of said Benes network.

11. The method according to claim 10 wherein said permutation instruction comprises a reference to two configuration registers, and four stages of said Benes network are used.

12. The method of claim 1 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of bits, each said subword comprising one or more bits, and m is the number of network stages performed by one permutation instruction.

13. The method of claim 1 wherein said programmable processor is a microprocessor, digital signal processor, media processor, multimedia processor, cryptographic processor, or programmable System-on-a-Chip(SOC).

14. The method of claim 1 wherein said source sequence of bits is formed in subwords of two or more of said bits and further comprising the steps of:

after step c, determining pass through stages in said Benes network; and

eliminating said pass through stages.

15. A method of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising the steps of:

a. defining an intermediate sequence of bits that said source sequence of bits is transformed into with a configuration of a Benes network;

b. determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits;

c. storing said determined intermediate sequence of bits; and

d. determining a subsequent permutation instruction using said stored intermediate sequence of bits.

16. The method of claim 15 further comprising repeating step c. and d. until a desired sequence of bits is obtained,

wherein the determined permutation instructions form a permutation instruction sequence.

17. A method of performing an arbitrary permutation of a source sequence of bits in a programmable processor said source sequence of bits is packed into a plurality of source registers comprising the steps of:

a. dividing bits of a first of said source registers to be placed in a first destination register into a first group and bits of said first of said source registers to be placed in a second destination register into a second group with a first permutation instruction sequence;

b. dividing bits of a second of said source registers to be placed in said first destination register into a first group and bits of said second of said source registers to be placed in a second destination register into a second group with a second permutation instruction sequence;

c. placing bits of said first group of said first of said source registers and said bits of said first group of said second of said source registers into said first destination register;

d. placing bits of said second group of said first of said source registers and said second group of said second of said registers into said second destination register;

e. defining a sequence of bits of said first destination register as a first source sequence of bits and a sequence of bits of said second destination register as a second source sequence of bits;

f. defining an intermediate sequence of bits that each of said first source sequence of bits and said second source sequence of bits is transformed into using a Benes network;

g. determining a permutation instruction for transforming said first source sequence of bits and said second source sequence of bits into respective said intermediate sequence of bits; and

h. repeating steps f. and g. using said determined intermediate sequence of bits from step g. as said source sequence of bits in step e. until a respective desired sequence of bits is obtained for said first source sequence of bits and said second source sequence of bits,

wherein the determined permutation instructions form a permutation instruction sequence.

18. The method of claim 17 wherein said programmable processor is a microprocessor, digital signal processor, media processor, multimedia processor, cryptographic processor, or programmable System-on-a-Chip(SOC).

19. The method of claim 17 wherein at most $4\lg n+2$ instructions are included in said permutation instruction sequence, wherein n is the number of subwords in said sequence of bits, each said subword comprising one or more bits.

20. The method of claim 1 wherein said permutation is reversed by the steps of reversing an order of each of said stages in said Benes network.

21. A method for performing a permutation of a source sequence of bits in a programmable processor comprising the steps of:

defining an intermediate sequence of bits that said source sequence of bits is transferred into using an Benes network; and

determining a sequence of one or more permutation instructions for transferring said source sequence of bits into said intermediate sequence of bits and optionally one or more subsequent intermediate sequences of bits until a desired sequence of bits is obtained.

22. The method of claim 1 wherein said Benes network comprises two butterfly networks of the same size connected back-to-back.

23. The method of claim 22 wherein said permutation instruction is assigned to two or more stages of said Benes network.

24. A system of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising:

means for defining an intermediate sequence of bits that said source sequence of bits is transformed into using Benes network stages; and

means for determining a permutation instruction for transforming said source sequence of bits into one or more intermediate sequence of bits until a desired sequence of bits is obtained,

wherein each intermediate sequence of bits is used as input to a subsequent permutation instruction and the determined permutation instructions form a permutation instruction sequence.

25. The system of claim 24 wherein the permutation instruction comprises an opcode indicating the configuration of said Benes network, a reference to a source register which contains said source sequence of bits, a reference to one or more configuration registers which contains configuration bits, and optionally a reference to a destination register to which said intermediate sequence of bits or said desired sequence of bits is placed.

26. The system of claim 25 wherein said opcode comprises a set of parameters, a first parameter indicating a first basic operation and a second parameter indicating a second basic operation.

27. The system of claim 26 wherein said first basic operation is specified by parameter m_1, wherein $2^{m}{}_1$ is a distance between conflict pairs of a stage of said Benes and said second basic operation is specified by parameter m_2, wherein 2^{m_2} is a distance between conflict pairs of a stage of said Benes network.

28. The system of claim 25 including a plurality of sets of configuration bits, wherein a first set of said configuration bits determines movement of said source sequence of bits in said source register to said intermediate sequence of bits during said first operation and a second set of said configuration bits determines movement of said intermediate sequence of bits into said destination register or a second intermediate sequence of bits during said second operation.

29. The system of claim 27 wherein a first set of said configuration bits determines movement of said source sequence of bits in said source register to said intermediate sequence of bits and a second set of a subsequent intermediate sequence of bits or said configuration bits determines movement of said intermediate sequence of bits into said destination register.

30. The system of claim 29 wherein each of said configuration bits is applied to a pair of conflict outputs of said Benes network.

31. The system of claim 30 wherein said first basic operation is specified by parameter m_1, wherein $2^{m}{}_1$ is a distance between conflict pairs of a stage of said Benes network and said second basic operation is specified by parameter m_2, wherein $2^{m}{}_2$ is a distance between conflict pairs of a stage of said Benes network.

32. The system of claim 24 wherein said permutation instruction is assigned to a pair of stages of said Benes network.

33. The system according to claim 24 wherein said permutation instruction comprises a reference to two configuration registers, andfour stages of said Benes network are used.

34. The system of claim 24 further comprising means for reversing an order of each of said stages in said Benes network.

35. The system of claim 24 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of subwords in said sequence of bits, each said subword comprising one or more bits, and m is the number of network stages performed by one permutation instruction.

36. The system of claim 24 wherein said programmable processor is a microprocessor, digital signal processor, media processor, multimedia processor, cryptographic processor, or programmable System-on-a-Chip(SOC).

37. The system of claim 24 wherein said source sequence of bits is formed in subwords of two or more of said bits and further comprising:

means for determining pass through stages in said Benes network; and

means for eliminating said pass through stages.

38. A system of performing an arbitrary permutation of a source sequence of bits in a programmable processor said source sequence of bits is packed into a plurality of source registers comprising:

means for dividing bits of a first of said source registers to be placed in a first destination register into a first group and bits of said first of said source registers to be placed in a second destination register into a second group with one said permutation instruction sequence;

means for dividing bits of a second of said source registers going to said first destination register into a first group and bits of a second of said source registers going to a second destination register into a second group with one said permutation instruction sequence;

means for placing bits of said first group of said first of said source registers and said bits of said first group of said second of said source registers into said first destination register;

means for placing bits of said second group of said first of said source registers and said second group of said second of said source registers into said second destination register;

means for defining a sequence of bits of said first destination register, as a first source sequence of bits and a sequence of bits of said second destination register as a second source sequence of bits;

means for defining an intermediate sequence of bits that each of said first source sequence of bits and said second source sequence of bits is transformed into using a Benes network; and

means for determining a permutation instruction for transforming said first source sequence of bits and said second source sequence of bits into one or more respective said intermediate sequence of bits until a respective desired sequence of bits is obtained for said first source sequence of bits and said second source sequence of bits,

wherein each intermediate sequence of bits is used as input to the subsequent permutation instruction and the determined permutation instructions form a permutation instruction sequence.

39. The system of claim 38 wherein at most $4\lg n+2$ instructions are included in said permutation instruction sequence, wherein n is the number of subwords in said sequence of bits, each said subword comprising one or more bits.

40. A system of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising:

means for defining an intermediate sequence of bits that said source sequence of bits is transformed into with a configuration of a Benes network;

means for determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits;

means for storing said determined intermediate sequence of bits; and

means for determining a subsequent permutation instruction using said stored intermediate sequence of bits.

41. A system for performing a permutation of a source sequence of bits in a programmable processor comprising:

means for defining an intermediate sequence of bits that said source sequence of bits is transformed into using Benes network stages; and

means for determining a sequence of permutation operations for transforming said source sequence of bits into one or more intermediate sequence of bits until a desired sequence of bits is obtained.

42. The system of claim 41 wherein said intermediate sequence of bits is determined with a configuration of an Benes network, said Benes network comprising two butterfly networks of the same size connected back-to-back.

43. The system of claim 42 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of bits, each said subword comprising one or more bits, and m is the number of network stages performed by one permutation instruction.

44. A computer implemented method for performing an arbitrary permutation of a sequence of bits comprising the steps of:

inputting said sequence of bits into a source register;

connecting said source register to an Benes network;

in response to an CROSS instruction selecting a configuration of said network; and

moving each of said bits in said source register to a position in a sequence of bits of a destination register based on configuration bits of a configuration register.

45. The method of claim 44 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of subwords in said sequence of bits, each said subword comprising one or more bits, and m is the number of network stages performed by one permutation instruction.

46. A computer system for performing an arbitrary permutation comprising:

a source register;

a configuration register;

a destination register;

a Benes network coupled to said first source register, said configuration register and said destination register, in response to a CROSS instruction selecting a configuration of said Benes network, placing each bit in said sequence of bits from said source register to a position in a sequence of bits in said destination register based on a configuration of bits of said configuration register.

47. The system of claim 46 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of subwords in said sequence of bits, each said subword comprising one or more bits, and m is the number of network stages performed by one permutation instruction.

48. The system of claim 47 wherein said intermediate sequence of bits is determined with a configuration of an Benes network, said Benes network comprising two butterfly networks of the same size connected back-to-back.

49. A computer readable medium having stored thereon data representing a sequence of permutation instructions, the sequence of permutation instructions which when executed by a processor, cause the processor to permutate a source sequence of subwords into one or more intermediate sequences of subwords using a Benes network, each intermediate sequence of subwords using input from said source sequence of subwords or a previous said intermediate sequence of subwords until a desired sequence of subwords is obtained, wherein each subword is one or more bits.

50. The computer readable medium of claim 49 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of subwords in said sequence of bits, each said subword comprising one or more bits, and m is the number of network stages performed by one permutation instruction.

51. The system of claim 50 wherein said intermediate sequence of bits is determined with a configuration of an Benes network, said Benes network comprising two butterfly networks of the same size connected back-to-back.

52. A cryptographic system, having stored thereon data representing a sequence of permutation instructions, the sequence of permutation instructions which when executed by a processor, cause the processor to permutate a source sequence of subwords into one or more intermediate sequences of subwords using a Benes network, each intermediate sequence of subwords using input from said source sequence of subwords or a previous said intermediate sequence of subwords until a desired sequence of subwords is obtained, wherein each subword is one or more bits.

53. The cryptographic system of claim 52 wherein at most $2\lg r/m$ said permutation instructions are included in said permutation instruction sequence, wherein r is the number of subwords in said sequence of subwords in said sequence of bits, each said subword comprising

one or more bits, and m is the number of network stages performed by one permutation instruction.

54. The system of claim 52 wherein said intermediate sequence of bits is determined with a configuration of an Benes network, said Benes network comprising two butterfly networks of the same size connected back-to-back.

55. A method of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising the steps of:

a. defining an intermediate sequence of bits that said source sequence of bits is transformed into with a configuration of a Benes network, said Benes network comprising at least two stages;

b. determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits;

c. storing said determined intermediate sequence of bits; and

d. determining a subsequent permutation instruction using said stored intermediate sequence of bits.

56. The method of claim 55 further comprising repeating step c. and step d. until a desired sequence of bits is obtained,

wherein the determined permutation instructions form a permutation instruction sequence.

57. The method of claim 56 wherein configuration bits are used in said permutation instruction for determining movement of said source sequence of bits in said source register to said intermediate sequence of bits or movement of said intermediate sequence of bits into a destination register or a second intermediate sequence of bits and two configuration registers are used for storing said configuration bits.

58. A system of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising:

means for defining an intermediate sequence of bits that said source sequence of bits is transformed into using Benes network stages;

means for determining a permutation instruction for transforming said source sequence of bits into one or more intermediate sequence of bits until a desired sequence of bits is obtained, wherein each intermediate sequence of bits is used as input to a subsequent permutation instruction and the determined permutation instructions form a permutation instruction sequence; and

means for reversing an order of each of said stages in said Benes network.

59. A system for performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising:

a. means for defining an intermediate sequence of bits that said source sequence of bits is transformed into with a configuration of a Benes network, said Benes network comprising at least two stages;

b. means for determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits;

c. means for storing said determined intermediate sequence of bits; and

d. means for determining a subsequent permutation instruction using said stored intermediate sequence of bits.

60. The system of claim 59 further comprising means for repeating c. and d. until a desired sequence of bits is obtained,

wherein the determined permutation instructions form a permutation instruction sequence.

61. The system of claim 60 wherein configuration bits are used in said permutation instruction for determining movement of said source sequence of bits in said source register to said intermediate sequence of bits or movement of said intermediate sequence

of bits into a destination register or a second intermediate sequence of bits and two configuration registers are used for storing said configuration bits.

62. A method of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising the steps of:

a. defining an intermediate sequence of bits that said source sequence of bits is transformed into;

b. determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits;

c. repeating steps a. and b. using said determined intermediate sequence of bits from step b. as said source sequence of bits in step a. until a desired sequence of bits is obtained, the determined permutation instructions form a permutation instruction sequence and configuration bits are used in said permutation instruction for determining movement of said source sequence of bits in a source register to said intermediate sequence of bits or movement of said intermediate sequence of bits into a destination register or a second intermediate sequence of bits;

d. storing said configuration bits; and

e. retrieving said stored configuration bits.

63. A method of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising the steps of:

a. defining an intermediate sequence of bits that said source sequence of bits is transformed into;

b. determining a permutation instruction for transforming said source sequence of bits into said intermediate sequence of bits;

c. repeating steps a. and b. using said determined intermediate sequence of bits from step b. as said source sequence of bits in step a. until a desired sequence of bits is obtained, the determined permutation instructions form a permutation instruction sequence and configuration bits are used in said permutation instruction for determining movement of said source sequence of bits in a source register to said intermediate sequence of bits or movement of said intermediate sequence of bits into a destination register or a second intermediate sequence of bits;

d. storing a portion of said configuration bits; and

e. retrieving said stored configuration bits.

64. A system of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising:

means for defining an intermediate sequence of bits that said source sequence of bits is transformed into using omega network stages and flip network stages;

means for determining a permutation instruction for transforming said source sequence of bits into one or more intermediate sequence of bits until a desired sequence of bits is obtained, wherein each intermediate sequence of bits is used as input to the subsequent permutation instruction and the determined permutation instructions form a permutation instruction sequence and configuration bits are used in said permutation instruction for determining movement of said source sequence of bits in said source register to said intermediate sequence of bits or movement of said intermediate sequence of bits into a destination register or a source register; and

means for storing said configuration bits and means for retrieving said stored configuration bits for use in said permutation instruction.

65. A system of performing an arbitrary permutation of a source sequence of bits in a programmable processor comprising:

means for defining an intermediate sequence of bits that said source sequence of bits is transformed into using Benes network stages and flip network stages;

means for determining a permutation instruction for transforming said source sequence of bits into one or more intermediate sequence of bits until a desired sequence of bits is obtained, wherein each intermediate sequence of bits is used as input to the subsequent permutation instruction and the determined permutation instructions form a permutation instruction sequence and configuration bits are used in said permutation instruction for determining movement of said source sequence of bits in said source register to said intermediate sequence of bits or movement of said intermediate sequence of bits into a destination register or a source register; and

means for storing said configuration bits and means for retrieving said stored configuration bits for use in said permutation instruction.